ON THE SOLUTIONS OF DECOMPOSABLE FORM EQUATIONS (New Aspects of Analytic Number Theory)

AUTHOR(S):

Gyory, Kalman

CITATION:

Gyory, Kalman. ON THE SOLUTIONS OF DECOMPOSABLE FORM EQUATIONS (New Aspects of Analytic Number Theory). 数理解析研究所講究録 2002, 1274: 142-156

ISSUE DATE:

2002-07

URL:

http://hdl.handle.net/2433/42258

数理解析研究所講究録 1274 巻 2002 年 142-156

ON THE SOLUTIONS OF DECOMPOSABLE FORM EQUATIONS

K.GYŐRY (Debrecen)

A homogeneous polynomial $F(\underline{x}) = F(x_1, \dots, x_m)$ with integer coefficients is called decomposable if it factorizes into linear forms with algebraic coefficients. Then the equation

$$(1) \qquad F(\underline{x}) = F(x_1, \dots, x_m) = \pm a \quad \text{in} \quad \underline{x} \in \mathbb{Z}^m,$$

where a is a given non-zero integer, is called a decomposable form equation. We assume throughout this paper that F contains m linearly independent linear factors.

The most important types of decomposable form equations are the

Pell equations: $x_1^2 - dx_2^2 = \pm 1$, where $d > 1$ is a square-free integer;

Thue equations, where $m = 2$, $\deg F \geq 3$ and F is irreducible over $\mathbb{Q}$;

norm form equations, when $m \geq 2$ and F is irreducible over $\mathbb{Q}$;

discriminant form equations and **index form equations.**

These equations have a lot of important applications, among others to other diophantine equations, algebraic number theory, linear recurrence sequences, irreducible polynomials, polynomials of given discriminant or of given resultant, canonical number systems, prime divisors of numbers of the form $a+b$ and $ab+1$, and units of integral group rings.

There is an extremely extensive literature of these equations; several books and hundreds of papers are concerned with decomposable form equations and their applications. In our paper we give a short survey of the most significant results obtained over the past ten years. For more detailed overviews of the subject we refer to the recent works of Schmidt(1990) and Győry (1998,1999,2000).

In the first part we deal with general (but ineffective) finiteness results and, when the number of solutions is infinite, with the structure of the set of solutions. Part II is

devoted to effective finiteness results, while in the last part some numerical results will be presented. We shall mainly concentrate on equations in $m > 2$ unknowns. Further, we do not deal with decomposable form inequalities. For simplicity, results will be presented in their simplest forms, over the ring of integers $\mathbb{Z}$ and we shall only indicate extensions to the case of more general ground rings.

I. FINITENESS RESULTS, THE STRUCTURE OF THE SET OF SOLUTIONS

1) Special decomposable form equations

Pell equations can be written in the form

$$N_{K/\mathbb{Q}}(x_1 + \sqrt{d}\, x_2) = \pm 1 \quad \text{in} \quad x_1, x_2 \in \mathbb{Z},$$

where $K = \mathbb{Q}(\sqrt{d})$ and $d > 1$ is a square-free integer. As is known, the general solution is given by

$$x_1 + \sqrt{d}\, x_2 = \pm \varepsilon^a,$$

where ε is a fundamental unit in $\mathbb{Z}[\sqrt{d}]$, and $a \in \mathbb{Z}$ is arbitrary.

Thue equations are of the form

$$F(x_1, x_2) = \pm a \quad \text{in} \quad x_1, x_2 \in \mathbb{Z}, \tag{2}$$

where $F \in \mathbb{Z}[x_1, x_2]$ is an irreducible binary form with degree ≥ 3.

THEOREM A (Thue, 1909). Equation (2) has only finitely many solutions.

Similar results over more general ground rings and quantitative versions providing bounds for the number of solutions were later obtained by Siegel, Mahler, Lang, Davenport and Roth, Lewis and Mahler, Schinzel, Evertse, Silverman, Bombieri and Schmidt, Evertse and Győry, Stewart, Brindza, Győry and others. The proofs of these results are mostly based on the Thue-Siegel-

Roth diophantine approximation method and its various generalizations. This method is ineffective, i.e. do not provide any algorithm for determining the solutions of (2).

Norm form equations. Let K be an algebraic number field of degree $n \geq 2$, and let $\alpha_1 = 1, \alpha_2, \ldots, \alpha_n$ be linearly independent elements of K over $\mathbb{Q}$ such that $K = \mathbb{Q}(\alpha_2, \ldots, \alpha_n)$. Consider the norm form equation

$$(3) \qquad c N_{K/\mathbb{Q}}(\alpha_1 x_1 + \cdots + \alpha_n x_n) = \pm a \quad \text{in } x_i \in \mathbb{Z},$$

where c is a non-zero rational number such that the norm form $c N_{K/\mathbb{Q}}(\alpha_1 x_1 + \cdots + \alpha_n x_n)$ has its coefficients in $\mathbb{Z}$. For $n \geq 3$, $n = 2$, (3) is just a Thue equation.

The $\mathbb{Z}$-module $\mathcal{M} = \{\alpha_1, \ldots, \alpha_n\}$ is called degenerate if there exist a $\mu \in K^*$ and a subfield L of K having infinitely many units (i.e., L is different from $\mathbb{Q}$ and the imaginary quadratic fields) such that $\mu L \subseteq \mathcal{M}$. It is known that if $\mathcal{M}$ is degenerate then there is a non-zero $a \in \mathbb{Z}$ for which (3) has infinitely many solutions. As a generalization of Thue's theorem, Schmidt proved the following.

THEOREM B (W.Schmidt,1971). *If $\mathcal{M}$ is non-degenerate, then equation (3) has only finitely many solutions for all non-zero $a \in \mathbb{Z}$.*

Moreover, Schmidt (1972) described in full generality the structure of the set of solutions of (3). This will be presented later in a more general form.

Extensions to the case of more general ground rings and bounds for the number of solutions were later established by Schmidt, Schlickewei Laurent, Evertse and Győry, Győry, Evertse, Voutier and Bérczes. The main tool in the proofs were Schmidt's Subspace Theorem as well as its generalizations and quantitative versions.

Discriminant form and index form equations. Let again K be a number field of degree $n \geq 3$ with discriminant D_K, ring of integers $\mathcal{O}_K$, and integral basis $\{1, \alpha_2, \ldots, \alpha_n\}$. For $\alpha = x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n$ with $x_i \in \mathbb{Z}$, we have

$$D_{K/\mathbb{Q}}(\alpha_2 x_2 + \dots + \alpha_n x_n) = (I(x_2, \dots, x_n))^2 D_K$$

and $|I(x_2, \dots, x_n)| = [O_K^+ : \mathbb{Z}[\alpha]^+]$. The decomposable forms $D_{K/\mathbb{Q}}(\alpha_2 x_2 + \dots + \alpha_n x_n)$ and $I(x_2, \dots, x_n)$ are called <u>discriminant form</u> and <u>index form</u>, while the equations

$$(4) \qquad D_{K/\mathbb{Q}}(\alpha_2 x_2 + \dots + \alpha_n x_n) = \pm a \quad \text{in } x_2, \dots, x_n \in \mathbb{Z}$$

and

$$(5) \qquad I(x_2, \dots, x_n) = \pm I \quad \text{in } x_2, \dots, x_n \in \mathbb{Z}$$

are called <u>discriminant form equation</u> and <u>index form equation</u>, respectively.

Example: For $K = \mathbb{Q}(\sqrt[3]{d})$, where $d \neq$ full cube, one has

$$D_{K/\mathbb{Q}}(\sqrt[3]{d}\, x_2 + \sqrt[3]{d^2} x_3) = -27 d^2 (x_2^3 - d x_3^3)^2.$$

For $n \leq 4$, Nagell, Delone, and Delone and Faddeev proved, in an ineffective form, the finiteness of the number of solutions of (4) and (5).

THEOREM C (Győry, 1976). <u>Equations (4) and (5) have only finitely many solutions, and all them can be effectively determined.</u>

Extensions to the case of more general ground rings and bounds for the number of solutions were later given by Győry and Papp, Trelina, Győry, Evertse and Győry, and Bérczes.

2) <u>Description of the structure of the set of solutions; general case</u>

Consider now the general decomposable form equation (1). In (1), the decomposable form F can be written in the form

$$F(\underline{x}) = c \prod_{i=1}^{t} N_{K_i/\mathbb{Q}}(l_i(\underline{x})),$$

where the K_i are appropriate number fields, the l_i are linear forms with coefficients in K_i, and c is a fixed non-zero

rational number. For $t = 1$, (1) is just a norm form equation.

In the $\mathbb{Q}$ -algebra $A = K_1 \oplus \dots \oplus K_t$, the algebra norm of $\alpha = (\alpha_1, \dots, \alpha_t) \in A$ has the property

$$N_{A/\mathbb{Q}}(\alpha) = \prod_{i=1}^{t} N_{K_i/\mathbb{Q}}(\alpha_i).$$

Let

$$(6) \qquad \mathcal{M} := \{ x = (l_1(\underline{x}), \dots, l_t(\underline{x})) \in A : \underline{x} \in \mathbb{Z}^m \}.$$

Then (1) can be reformulated as

$$(1') \qquad c N_{A/\mathbb{Q}}(x) = \pm a \text{ in } x \in \mathcal{M}.$$

For a subalgebra B of A with $1_A = (1, \dots, 1) \in B$, let O_B denote the integral closure of $\mathbb{Z}$ in B , and O_B^* the unit group in O_B . Put $V := \mathcal{M}\mathbb{Q}$, and

$$V^B := \{ v \in V : vB \subseteq V \} , \quad \mathcal{M}^B := V^B \cap \mathcal{M}.$$

Then

$$U_{\mathcal{M},B} := \{ \varepsilon \in O_B^* : \varepsilon \mathcal{M}^B = \mathcal{M}^B \}$$

is a subgroup of finite index in O_B^* . If $x \in \mathcal{M}^B$ is a solution of (1') , then so is every element of $x U_{\mathcal{M},B}$. This set $x U_{\mathcal{M},B}$ is called an $(\mathcal{M}, B)$ -family of solutions of (1'). It is called maximal if is not properly contained in another family. Further, rank $U_{\mathcal{M},B}$ is called the rank of the family $x U_{\mathcal{M},B}$.

THEOREM D (Győry, 1993). The set of solutions of (1') is the union of finitely many families of solutions. Further, there are only finitely many maximal families of solutions.

Moreover, in Győry(1993) an explicit upper bound has been given for the number of maximal families. These include (in an ineffective form) all the above-mentioned finiteness results on special decomposable form equations.

The proof is long and difficult. Equation (1) is first reduced to unit equation systems. The remaining part of the proof depends among other things on a quantitative version of

the Subspace Theorem.

As a consequence of Theorem D, we proved with Everest(1997) that if (1) has infinitely many solutions, then the counting function

$$P(N) := \#\{\underline{x} \in \mathbb{Z}^m : (1)\ F(\underline{x}) = \pm a,\ |\underline{x}| \leq N\}$$

satisfies

$$P(N) = \gamma (\log N)^t + O((\log N)^{t-1}),$$

where $\gamma > 0$ is constant, and t denotes the maximal rank of the families of solutions of (1'). This includes as special cases some earlier results of Lang, Babaev, and Győry and Pethő on special decomposable form equations.

Recently, Everest,Gaál, Győry and Röttger described the spatial distribution of the solutions $\underline{x}$ of (1), more precisely the distribution of $\underline{x}/|\underline{x}|$.

3) Finiteness criterion; general case

Consider again equation (1) and its reformulation (1'). The $\mathbb{Z}$-module M defined by (6) is called degenerate if there is a $\mu \in A^*$ and a subalgebra B of A with infinitely many units such that $\mu B \subset M\mathbb{Q}$. As a consequence of Theorem D, I proved the following general criterion.

THEOREM E (Győry,1993). **The equation (1) $\Leftrightarrow$ (1') has only finitely many solutions for every non-zero $a \in \mathbb{Z}$ if and only if M is non-degenerate.**

For $t = 1$, this gives Schmidt's Theorem B on norm form equations. Theorem E was proved in a more general form, over finitely generated subrings of $\overline{\mathbb{Q}}$ over $\mathbb{Z}$. Further, in case of finitely many solutions, an explicit upper bound was given for the number of solutions.

The upper bound for the number of solutions was later improved by Evertse, and Evertse and the author. The best known upper bound is as follows.

THEOREM F (Evertse and Győry, 1997). If equation (1) has finitely many solutions, then this number does not exceed

$$(7) \qquad (2^{33} n^2)^{e(m)(\omega(a)+1)}$$

where $n = \deg F$, $\omega(a)$ denotes the number of distinct prime factors of a, and $e(m) = \frac{1}{3} m(m+1)(2m+1) - 2 \ (\leq m^3)$.

4) Generalizations to decomposable polynomial equations, bounds for the number of solutions

Let now $F \in \mathbb{Z}[\underline{x}]$ be a decomposable polynomial, i.e. suppose that F factorizes into linear (not necessarily homogeneous) polynomials $l_1, \ldots, l_n$ over $\overline{\mathbb{Q}}$. Assume that $\operatorname{rank}\{l_1, \ldots, l_n\} = m+1$.

Let S denote a finite set of primes $\{p_1, \ldots, p_s\}$, let $\mathbb{Z}_S$ be the ring of S-integers, and $\mathbb{Z}_S^*$ the group of S-units.

THEOREM G (Bérczes and Győry, 2002). If the number of solutions of the decomposable polynomial equation

$$(1a) \qquad F(\underline{x}) = F(x_1, \ldots, x_m) \in \mathbb{Z}_S^* \ \text{ in } \ \underline{x} \in \mathbb{Z}_S^m$$

is finite, then this number does not exceed

$$(8) \qquad (2^{33} n^2)^{e(m+1)(s+1)}.$$

(7) and (8) give uniform explicit bounds for the numbers of solutions of norm form, discriminant form and index form equations and of their "inhomogeneous" generalizations, subject only to the condition that the number of solutions is finite. It should be observed that the bounds obtained are independent of the coefficients of F.

Theorem G makes explicit a result of Evertse, Gaál and Győry (1989) on decomposable polynomial equations, and generalizes, with $e(m+1)$ instead of $e(m)$, the Theorem F of Evertse and Győry (1997) on decomposable form equations.

We note that (8) is not far from being best possible in terms of s. Indeed, Evertse, Moree, Stewart and Tijdeman (2oo?) gave for each $n \geq 3$, $2 \leq m \leq n-1$ and sufficiently large s, an example for equation (1a) with more than

$$\exp\{c s^{m/n} (\log s)^{(m/n)-1}\}$$

solutions.

Theorems E, F and G have many applications, among others to irreducible polynomials (Győry,1994), to prime divisors of integers of the form $a+b$ and $ab+1$ (Győry, Sárközy and Stewart,1996), and to resultant equations (Bérczes and Győry, 2oo2).

II. EFFECTIVE FINITENESS RESULTS

Thue equations

Consider again the Thue equation (2), where $F \in \mathbb{Z}[x_1, x_2]$ is an irreducible binary form of degree $n \geq 3$ with height H. Using his fundamental results concerning linear forms in logarithms, A.Baker gave the first effective version of Thue's theorem.

THEOREM H (Baker,1968). *All solutions x_1, x_2 of (2) satisfy*

$$\max(|x_1|, |x_2|) < \exp\{n^{\nu^2} H^{\nu n^3} + (\log|a|)^{2n+2}\},$$

where $\nu = 128\, n(n+1)$.

For Thue equations, this gave a positive answer to Hilbert's 1oth problem. Theorem H was improved and generalized to the case of more general ground rings by many people, including Baker, Sprindžuk, Coates, Feldman, Stark, Győry and Papp. The best known bound is due to Bugeaud and Győry (1996).

Let $K = \mathbb{Q}(\alpha)$, where $F(\alpha, 1) = 0$. Denote by R_K the regulator of K.

THEOREM I (Bugeaud and Győry,1996). *All solutions of (2) satisfy*

$$\max(|x_1|, |x_2|) < c_1 (H \cdot |a|)^{c_2}, \tag{9}$$

where

$$c_2 = n^{15(n+1)} R_K (\log R_K), \quad c_1 = \exp\{c_2 R_K\}.$$

It is an open question whether there exist c_1, c_2 depending only on n for which (9) holds.

In the proof the first main step is to reduce (2) to inequalities of the form

$$(10) \qquad 0 < |a_1 \log \varepsilon_1 + \dots + a_t \log \varepsilon_t - \log \beta| < e^{-\delta A},$$

where $\varepsilon_1, \dots, \varepsilon_t, \beta$ are fixed non-zero algebraic numbers, $a_i \in \mathbb{Z}$ are unknowns with $A = \max_i |a_i|$, and $\delta > 0$ is a constant. Then Baker's method gives an explicit upper bound A_0 for A which leads to a bound for $\max(|x_1|, |x_2|)$.

Recently Bombieri, and Bombieri and Cohen have developed a new effective method in diophantine approximation which provides almost the same bounds for the number of solutions of (2) as those obtained by Baker's theory concerning linear forms in logarithms.

Discriminant form and index form equations

Let K be a number field of degree $n \geq 3$ with discriminant D_K, ring of integers O_K and integral basis $\{\alpha_1 = 1, \alpha_2, \dots, \alpha_n\}$ with $\max_i |\alpha_i| \leq A$.

By Theorem C of Győry presented above, equations (4) and (5) have only finitely many solutions. Further, in Győry (1976) explicit upper bounds were given for the solutions, which bounds depend only on A, n, D_K and $|a|$ and $|I|$, respectively. This theorem yielded many **consequences** and **applications**. Let me mention some of them.

- Up to translation by elements of $\mathbb{Z}$, there are only finitely many $\alpha \in O_K$ with a given non-zero discriminant, and all them can be effectively determined (Győry, 1976). This confirmed, in an effective form, a conjecture of Nagell.
- Up to translation of the form $f(x) \to f(x+a)$ $(a \in \mathbb{Z})$, there are only finitely many monic $f \in \mathbb{Z}[x]$ with a given non-zero discriminant, and all them can be effectively determined (Győry, 1976). This gave a positive answer to a problem of Delone and Faddeev.

- Up to translation by elements of $\mathbb{Z}$, there are only finitely many $\alpha \in \mathcal{O}_K$ such that $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Further, an explicit bound was given for the heights of α (Győry, 1976). This provided the solution of an old problem going back to the XIX century.
- An algorithm was given for the existence of canonical number systems in number fields (B.Kovács,1981,1984).

The main steps in the <u>proof</u> of Theorem C are as follows. Combining some methods from algebraic number theory, geometry of numbers and combinatorics, one can reduce equations (4) and (5) to systems of unit equations of the form

$$(11) \qquad \varrho_1 \varepsilon_1^{a_{11}} \cdots \varepsilon_t^{a_{1t}} + \varrho_2 \varepsilon_1^{a_{21}} \cdots \varepsilon_t^{a_{2t}} = 1,$$

where $\varepsilon_1, \ldots, \varepsilon_t$ are fundamental units in $K^{(i)}K^{(j)}K^{(l)}$ or in the normal closure of $K/\mathbb{Q}$, and $a_{ij} \in \mathbb{Z}$ are unknowns. Then one can reduce (11) to an inequality of the shape (10). Now Baker's method gives a bound for $\max_{i,j} |a_{ij}|$ which yields a bound for $\max_i |x_i|$.

Recently, I succeeded (Győry,1998,2000) to refine significantly the above method of proof by reducing (4) and (5) to unit equations over <u>much smaller</u> number fields (over appropriate subfields of $K^{(i)}K^{(j)}$). This led to smaller t and smaller other parameters involved, hence giving a <u>much better bound</u> for $\max_i |x_i|$.

THEOREM J (Győry,2000). <u>**All solutions**</u> $(x_2, \ldots, x_n) \in \mathbb{Z}^{n-1}$ <u>**of**</u> (4) <u>**satisfy**</u>

$$\max_i |x_i| < A^{n-2} \exp\{c\,|D_K|^{\frac{n-1}{2}} (\log |D_K|)^{n(n-1)} (|D_K|^{\frac{n-1}{2}} + \log |a|)\},$$

<u>**where**</u> $c = n^5 n_1^{8n_1+25}$ <u>**and**</u> $n_1 \le n(n-1)/2$.

On the other hand, the refinement mentioned above provided a much more efficient algorithm for the resolution of (4) and (5) in concrete cases.

Norm form equations and decomposable form equations of general type

Subject to some conditions concerning $\alpha_1, \ldots, \alpha_m$, effective

bounds for the solutions of the norm form equation (3) were given by Győry and Papp (1978), Győry (1981), Kotov (1981), Bugeaud and Győry (1996), Győry (1998) and, in the "inhomogeneous" case, by Gaál (1985).

In 1998 I proved (cf. Győry, 1998) that if α_m is of degree at least 3 over $\mathbb{Q}(\alpha_1,\dots,\alpha_{m-1})$, then all solutions of (3) with $x_m \neq 0$ satisfy

$$\max_i |x_i| < c_1 (A \cdot |a|)^{c_2},$$

where $\max_i |\alpha_i| \leq A$ and the constants $c_i = c_i(n, D_K)$, $i = 1, 2$, are explicitly given. It is easy to show that here the conditions concerning α_m and x_m are necessary.

In 1981 and 1998 I gave (cf. Győry, 1998) common generalizations of the above-presented effective results concerning Thue equations, discriminant form and index form equations, and norm form equations.

In the proof, the method applied earlier to discriminant form and index form equations was generalized in an appropriate way; see e.g. Győry (1998).

III. NUMERICAL RESULTS

Thue equations

The general bounds obtained for the solutions of Thue equations are too large for practical use in concrete cases.

Example: All solutions $x_1, x_2 \in \mathbb{Z}$ of the equation

$$x_1^4 - 4x_1^3x_2 - 6x_1^2x_2^2 + 4x_1x_2^3 + x_2^4 = 1 \text{ in } x_i \in \mathbb{Z} \tag{12}$$

satisfy

$$\max(|x_1|, |x_2|) < \exp\{10^{60}\}.$$

Further, one can deduce from (12) an inequality of the form

$$0 < |a_1 \log \varepsilon_1 + a_2 \log \varepsilon_2 + a_3 \log \varepsilon_3 - \log \beta| < e^{-\delta A},$$

where the $a_i \in \mathbb{Z}$ are unknowns and $A = \max_i |a_i|$. Then Baker's method gives $A < 10^{50}$ which is still too large for practical

In the last two decades many people, including Pethő, de Weger, Tzanakis, Mignotte, Wakabayashi, and Bilu-Hanrot developed efficient algorithms for the resolution of concrete Thue equations (see e.g. Bilu and Hanrot, 1996, and Smart, 1998). These algorithms consist of two main parts: one first reduces the bound on A (in several steps) by means of the Baker-Davenport's reduction method or by the LLL basis reduction algorithm. Then the remaining "small" vactors (a_i) are enumerated by using computer. There are currently computer packages, e.g. the KANT for performing various number theoretic calculations and providing all the solutions of Thue equations with $n = \deg F \le 20$ and with "small" $H(F)$ and $|a|$. For example, all solutions (x_1, x_2) of (12) are, up to sign, $(0,1), (1,0), (2,3), (3,2)$.

Index form equations

Index form equations (5) are of particular interest in the case when $I = 1$. If the index form in (5) is associated to the integral basis $\{1, \alpha_2, \dots, \alpha_n\}$ of a number field K, then, for $I = 1$, $(x_2, \dots, x_n) \in \mathbb{Z}^{n-1}$ is a solution of (5) if and only if $\alpha = x_1 + x_2\alpha_2 + \dots + x_n\alpha_n$ (for any $x_1 \in \mathbb{Z}$) satisfies $O_K = \mathbb{Z}[\alpha]$, i.e. if $\{1, \alpha, \dots, \alpha^{n-1}\}$ is a power integral basis of K.

For number fields of degree $n = 3$ and 4, Gaál, Schulte, Pethő, Pohst and Koppenhöfer gave efficient algorithms for solving (5) by reducing (5) to cubic and quartic Thue equations (see e.g. Smart, 1998). They determined the minimal I for which (5) is solvable, and gave all solutions in several hundred number fields. Some extensions were also established to some special number fields of degree $n = 6, 8, 9$. However, these methods do not work in general for number fields of degree $n = 5$.

Our **general method** (Győry, 1976) reduces (5) to unit equations of the form

$$(11) \qquad \eta_1 \varepsilon_1^{a_{11}} \dots \varepsilon_r^{a_{1r}} + \eta_2 \varepsilon_1^{a_{21}} \dots \varepsilon_r^{a_{2r}} = 1 \quad \text{in } a_{ij} \in \mathbb{Z} \text{ unknowns}$$

over $K^{(i)}K^{(j)}K^{(l)}$ or the normal closure of $K/\mathbb{Q}$, where

$$(13) \qquad r \le n(n-1)(n-2) - 1.$$

Baker's method can be used to derive a "large" upper bound A_0 for $A = \max_{i,j} |a_{ij}|$. Then, in concrete case, the reduction algorithms provide a much "smaller" bound A_1 for A. However, the number of remaining possibilities to enumerate is still in general about 200^{2r}, which is hopeless if r is large.

In special number fields K with "small" r Smart (1996) and Wildanger (1997) gave efficient algorithms for the enumeration of the "small" a_{ij} and hence for the resolution of (5). However, their methods do not work for the degrees $n = 4, 5$ if r is "large".

Our **refinement of the general method** (Győry, 2000) reduces (5) to equations (11) over a much smaller number field, an appropriate subfield of $K^{(i)}K^{(j)}$. This yields a significant improvement of (13):

$$r \le \frac{n(n-1)}{2} - 1. \tag{14}$$

Comparing (13) and (14) for $n = 5$, it is easily seen that the general method gives $r \le 59$, while its improvement yields $r \le 9$.

On combining the refined general method with Baker's method, the LLL reduction algorithm and Wildanger's algorithm, Gaál and Győry (1999) gave an efficient algorithm for the resolution of (5) for number fields K of degree 5.

Example (Gaál and Győry, 1999): Let $n = 5$, $K = \mathbb{Q}(\xi)$, ξ a root of $x^5 - 6x^3 + x^2 + 4x + 1 = 0$. Then $D_K = 36497$, $\{1, \xi, \xi^2, \xi^3, \xi^4\}$ is an integral basis of K, K is totally real, and the Galois group of K is S_5 (most difficult case !). Then, up to sign, all solutions $(x_2, x_3, x_4, x_5) \in \mathbb{Z}^4$ of the corresponding index form equation

$$I(x_2, x_3, x_4, x_5) = \pm 1$$

are:

$(1,-6,0,1), (1,0,0,0), (2,-6,0,1), (2,-5,0,1), (3,-11,0,2),$
$(3,-5,0,1), (3,0,-5,2), (4,-5,-1,1), (4,0,-3,-1), (4,5,-1,-1),$
$(6,-6,-1,1), (6,15,-2,-3), (7,-12,-1,2), (7,-11,-1,2), (8,-12,-1,2),$
$(9,-18,-1,3), (9,-17,-1,3), (11,-23,-1,4), (13,-18,-2,3),$
$(15,-24,-2,4), (16,-23,-2,4), (19,-41,-2,7), (31,-46,-4,8),$
$(53,62,-14,-13), (80,-159,-9,27), (115,-166,-15,29).$

Remark. In order to solve concrete index form equations in number fields of degree 6, it would be sufficient to give an efficient algorithm for enumerating the "small" solutions a_i in (11) for $r \leq 14$.

Acknowledgements. The author would like to express his gratitude to the organizers of the conference, to Professors Y. Tanigawa and S.Kanemitsu for their hospitality, and to the Nagoya University, the Kinki University and the Hungarian Academy of Sciences for their financial supports.

References

A.Baker (1968), Contributions to the theory of Diophantine equations, Philos.Trans.Roy.Soc.London A, 263,173-208.

A.Bérczes and K.Győry (2002), On the number of solutions of decomposable polynomial equations, Acta Arith. 101, 171-187.

Y.Bilu and G.Hanrot (1996), Solving Thue equations of high degree, J.Number Theory, 60,373-392.

Y.Bugeaud and K.Győry (1996), Bounds for the solutions of Thue-Mahler equations and norm form equations, Acta Arith. 74,273-292.

J.H.Evertse and K.Győry (1997), The number of families of solutions of decomposable form equations, Acta Arith. 80,367-394.

J.H.Evertse, P.Moree, C.L.Stewart and R.Tijdeman (200?), Multivariate Diophantine equations with many solutions, Acta Arith., to appear.

I.Gaál and K.Győry (1999), Index form equations in quintic fields, Acta Arith. 89,379-396.

K.Győry (1976), Sur les polynômes à coefficients entiers et de discriminant donné III, Publ.Math.Debrecen 23, 141-165.

K.Győry (1993), On the numbers of families of solutions of systems of decomposable form equations, Publ.Math. Debrecen 42,65-101.

K.Győry (1998), Recent bounds for the solutions of decomposable form equations, In: Number Theory, de Gruyter, 255-270.

K.Győry (1999), On the distribution of solutions of decomposable form equations, In: Number Theory in Progress, de Gruyter,237-265.

K.Győry (2ooo), Discriminant form and index form equations, In: Algebraic Number Theory and Diophantine Analysis, de Gruyter,191-214.

W.M.Schmidt (1971), Linearformen mit algebraischen Koeffizienten II, Math.Ann. 191,1-2o.

W.M.Schmidt (1972), Norm form equations, Ann. of Math. 96, 526-551.

W.M.Schmidt (199o), Diophantine approximations and diophantine equations, Lecture Notes in Math. 1467. Springer.

N.P.Smart (1998), The algorithmic resolution of diophantine equations, Cambridge University Press.

A.Thue (19o9), Über Annaherungswerte algebraischer Zahlen, J. Reine Angew.Math. 135,284-3o5.

Institute of Mathematics and Informatics
University of Debrecen
H-4olo Debrecen, Hungary
E-mail: gyory@math.klte.hu